Journal of Information and Communication Technology

Volume 16, Issue 61-62, Autumn and Winter 2024, pp. 205-217

Providing a Blockchain-Based Method to Protect Users' Privacy in Social Networks

Ibrahim Zamani Babgohari[1], Monireh Hosseini[2*]

[1] Department of Information Technology Engineering, KNTU, Tehran, Iran
[2] Department of Information Technology Engineering, KNTU, Tehran, Iran

Received: 27 August 2023, Revised: 11 May 2024, Accepted: 13 May 2024
Paper type: Research

Abstract

Today, social networks have brought a lot of convenience to their users, but there are still problems of not respecting privacy. This has caused the security and privacy protection of social network users to be important. Users share a large amount of personal data on social networks, attackers can obtain sensitive personal information simply by using social networks. and carry out various types of attacks and identity theft. Many social networks do not have their own data centers and usually store user data in third-party data centers. These centers can share this data with others and provide user data to other organizations without their knowledge. Owners of social networks can provide users' data to information agencies or use them for advertising purposes. In this research, in the first part, we have described the introduction of the subject, and then in the second part, we have discussed the literature on the subject, which is mostly focused on the centralized methods of privacy protection, and then in the third part, we have described the research method. And we have presented a method that increases the privacy of users in social networks to a great extent by using blockchain. In the fourth part, we have described the implementation of the research and finally we have concluded and summarized this research.

Keywords: Privacy, Information Security, Blockchain.

[*] Corresponding Author's email: hosseini@kntu.ac.ir

دوفصلنامه
فناوری اطلاعات و ارتباطات ایران

سال شانزدهم، شماره‌های ۶۱ و ۶۲، پاییز و زمستان ۱۴۰۳، صفحه ۲۰۵ الی ۲۱۷

ارائه روشی مبتنی بر بلاکچین برای حفظ حریم خصوصی کاربران در شبکه‌های اجتماعی

ابراهیم زمانی بابگهری[۱]، منیره حسینی[۲*]

[۱] گروه مهندسی فناوری اطلاعات، دانشگاه صنعتی خواجه نصیرالدین طوسی، تهران، ایران

[۲] گروه مهندسی فناوری اطلاعات، دانشگاه صنعتی خواجه نصیرالدین طوسی، تهران، ایران

تاریخ دریافت: ۱۴۰۲/۰۶/۰۵ تاریخ بازبینی: ۱۴۰۳/۰۲/۲۲ تاریخ پذیرش: ۱۴۰۳/۰۲/۲۴

نوع مقاله: پژوهشی

چکیده

امروزه شبکه‌های اجتماعی راحتی زیادی را برای کاربران خود به ارمغان آورده‌اند، اما هنوز مشکلات عدم رعایت حریم خصوصی وجود دارد. همین امر باعث شده امنیت و حفاظت از حریم خصوصی کاربران شبکه‌های اجتماعی مورد اهمیت قرار بگیرد. کاربران مقدار زیادی از داده‌های شخصی در شبکه‌های اجتماعی به اشتراک می‌گذارند، مهاجمان می‌توانند اطلاعات شخصی حساس را به سادگی با استفاده از شبکه‌های اجتماعی به دست آورند و انواع مختلفی از حملات و سرقت هویت را انجام دهند. بسیاری از شبکه‌های اجتماعی مراکز داده خود را ندارند و معمولاً داده‌های کاربر را در مراکز داده شخص ثالث ذخیره می‌کنند. این مراکز می‌توانند این داده‌ها را با سایرین اشتراک بگذارند و داده‌های کاربر را بدون اطلاع آنها در اختیار سازمان‌های دیگر قرار دهند. مالکان شبکه‌های اجتماعی می‌توانند داده‌های کاربران را در اختیار آژانس‌های اطلاعاتی قرار دهند و یا از آنها در زمینه‌های تبلیغاتی استفاده کنند. در این تحقیق در بخش اول مقدمه موضوع را شرح داده‌ایم و پس از آن در بخش دوم به ادبیات موضوع پرداخته‌ایم که بیشتر تمرکز کارهای قبلی بروی روش‌های متمرکز حفظ حریم خصوصی می‌باشد و سپس در بخش سوم روش تحقیق را شرح داده‌ایم و روشی را ارائه داده‌ایم که با استفاده از بلاکچین حریم خصوصی کاربران در شبکه‌های اجتماعی تا حد زیادی افزایش پیدا می‌کند. در بخش چهارم اجرای تحقیق را شرح داده‌ایم و در نهایت به نتیجه‌گیری و جمع‌بندی از این تحقیق پرداخته‌ایم.

واژه‌های کلیدی: حریم خصوصی، امنیت اطلاعات، بلاکچین.

* رایانامهٔ نویسنده مسؤول: hosseini@kntu.ac.ir

۱- مقدمه

شبکه‌های اجتماعی در دنیای امروز بسیار محبوب هستند. شبکه‌های اجتماعی به افراد اجازه می‌دهند تا با دوستان و خانواده خود ارتباط برقرار کنند و اطلاعات خصوصی خود را به اشتراک بگذارند. بدین خاطر مسائل مربوط به حفظ حریم خصوصی کاربر نمایان می‌شود. تعداد کاربران شبکه‌های اجتماعی در سراسر جهان هر ساله به طور مداوم در حال افزایش است[17]. براساس گزارش امنیتی سوفوس[1] در سال ۲۰۱۱[2]، فیس بوک ۰٫۵ میلیارد کاربر دارد اما در حال حاضر (2023) بیش از ۲٫۸ میلیارد کاربر دارد. این گزارش نشان می‌دهد که فیس بوک بزرگ‌ترین خطرات امنیتی را دارد که به طور قابل‌توجهی از مای اسپیس، توییتر، و لینکدین جلوتر است. این وب سایت محبوب‌ترین وب سایت برای کاربران فعال در وب است. با توجه به این محبوبیت، تعداد زیادی از کاربران توسط دشمنان از طریق انواع مختلفی از حملات مانند بدافزار، فیشینگ، اسپم‌نویسی و غیره مورد هدف قرار می‌گیرند این حملات به طور مداوم در حال افزایش هستند.

در جدول ۱ به تعاریفی پرداخته شده است که رعایت آنها باعث افزایش حفظ حریم خصوصی کاربران در شبکه‌های اجتماعی می‌شود. جدول ۲ مطالعات گذشته بر روی مسائل حریم خصوصی را نشان می‌دهد.

در این تحقیق با استفاده از بلاکچین و الگوریتم رمزنگاری بلوفیش روشی را برای افزایش حفظ حریم خصوصی کاربران در شبکه‌های اجتماعی ارائه می‌دهیم. در بخش دوم تحقیق به ادبیات موضوع می‌پردازیم و پس از آن در بخش سوم مدل را شرح می‌دهیم و سپس در بخش چهارم مدل را اجرا کرده و در نهایت در بخش پنجم به جمع‌بندی می‌پردازیم.

۲- ادبیات موضوع

در این بخش از تحقیق در جدول ۳ به مروری بر ادبیات موضوع می‌پردازیم.

جدول ۱. تعاریف موارد حفظ حریم خصوصی

مقاوم در برابر حملات اختلال سرویس	به معنای توانایی یک سیستم یا شبکه در مقابل حملات و اختلالات مختلف بوده و قادر به حفظ کارایی و عملکرد صحیح خود در مقابل این حملات باشد. این شامل حفظ دسترسی، حفظ امنیت و حفظ کارایی سرویس‌ها می‌شود.
جلوگیری از ذخیره داده در سرورها	به معنای اعمال سیاست‌ها یا محدودیت‌ها برای جلوگیری از ذخیره و نگهداری داده‌ها در سرورها است.
رمزگذاری داده‌ها	داده‌ها قبل از ذخیره‌سازی در پایگاه‌های داده به صورت رمزگذاری شده ذخیره می‌شوند.
حفاظت داده در برابر مالک شبکه اجتماعی	به معنای عدم توانایی دخالت مالکان شبکه‌های اجتماعی در داده‌های کاربران است.
محرمانه بودن داده‌ها	به معنای حفظ حریم خصوصی است. وقتی داده‌ها به عنوان محرمانه تشخیص داده می‌شوند، این به معنای این است که دسترسی به آنها تنها برای افراد یا سازمان‌های مجاز ممکن است.
اطلاعات درهم‌سازی شده	منظور هش است که یک تابع ریاضی است که یک ورودی را به یک مقدار خروجی ثابت و یکتا تبدیل می‌کند.
غیرمتمرکز بودن	شبکه‌هایی هستند که اطلاعات و ارتباطات بین کاربران بدون وابستگی به یک مرکز مشخصی انجام می‌شود.
تبادل کلید امن	به فرآیند تبادل کلیدهای رمزنگاری برای ایجاد ارتباط امن بین دو یا چند نهاد یا دستگاه می‌پردازد.
کنترل دسترسی دقیق	به مفهوم مدیریت و کنترل دسترسی به منابع و اطلاعات در یک سیستم یا شبکه است.
رمزگذاری سرتاسر	یک روش رمزنگاری است که در آن اطلاعات از زمان ارسال تا زمان دریافت، به صورت رمزنگاری شده باقی می‌مانند و تنها افرادی که دسترسی به کلید رمزگشایی دارند می‌توانند این اطلاعات را مشاهده کنند.

[1] Sophos
[2] https://tavaana.org/sites/default/files/

جدول ۲. مطالعات گذشته بر روی مسائل حفظ حریم خصوصی

شرح	منبع
یک سیستمی را با استفاده از فناوری تشخیص چهره ارائه داده‌اند در صورتی که کاربری رضایت نداشته باشد از اشتراک عکس، عکس آن در صورت به اشتراک گذاشته شدن به‌صورت بلوری و یا غیرقابل تشخیص نشان داده می‌شود. روش ارائه شده از نقص‌حریم خصوصی یک کاربر توسط کاربر دیگری جلوگیری می‌کند اما روش ارائه شده فاقد کارایی در مقابل نقص حریم‌خصوصی توسط مالک شبکه است. همین طور به دیگر ابعاد حفظ حریم‌خصوصی مانند مقاوم در برابر حملات اختلال سرویس، غیرمتمرکز بودن، تبادل کلید امن، کنترل دسترسی دقیق و... پرداخته نشده است.	[25]
یک طرحی ارائه شده است که با استفاده از الگوریتم‌های رمزنگاری به حفظ داده‌ها و افزایش حریم خصوصی کاربران در شبکه‌های اجتماعی می‌پردازد. اما در این طرح بعضی از ابعاد حفظ حریم‌خصوصی مانند مقاوم در برابر حملات اختلال سرویس، جلوگیری از ذخیره داده در سرورها، حفاظت داده در برابر مالک شبکه اجتماعی و ... پرداخته نشده است.	[26]
مسائل حفظ حریم خصوصی عمده در شبکه‌های اجتماعی را به چهار دسته تقسیم کرده‌اند: (الف) مسائل حریم خصوصی، (ب) بازاریابی ویروسی، (ج) حملات ساختاری شبکه و (د) حملات مخرب تحقیق آن‌ها شامل یک بحث عمیق در مورد هر موضوع و مکانیزم‌های دفاعی مربوطه بود.	[1]
مسائل امنیتی و حریم خصوصی کلی در شبکه‌های اجتماعی را مورد بررسی قرار داده‌اند و همین‌طور تکنیک‌های مختلفی را مورد بحث قرار دادند.	[17]
یک بررسی از تهدیدهای امنیتی و حریم خصوصی مختلف در شبکه‌های اجتماعی ارائه کرده است.	[2]
ارائه یک راهکار برای نبرد با حملات neighbors با استفاده از یک تکنیک دو مرحله‌ای جهت ناشناس سازی در شبکه‌های اجتماعی	[58]
سناریوهای مختلف مربوط به تهدیدات شبکه اجتماعی آنلاین و راه‌حل‌های آن‌ها را با استفاده از مدل‌ها، چارچوب‌ها و تکنیک‌های رمزگذاری مختلف ارائه کرده و با این کار از کاربران شبکه اجتماعی در برابر حملات مختلف محافظت می‌کند. علاوه براین راه‌حل‌های مختلف را مورد تجزیه و تحلیل قرار داده است.	[59]
به بررسی امنیت و حریم خصوصی در شبکه‌های اجتماعی می‌پردازد.	[60]
ارائه یک طبقه بندی در مورد چالش‌های حریم خصوصی و یک بررسی عمیق در مورد برخی از راه‌حل‌های ارائه شده اخیر در شبکه‌های اجتماعی.	[62]
به مروری برای پوشش تهدیدات ناشی از حریم خصوصی و امنیت اطلاعات در شبکه اجتماعی می‌پردازد و به صورت کلی حریم خصوصی را مورد بحث قرار می‌دهد، امنیت اطلاعات را با تمرکز بر تهدیدات مهندسی اجتماعی مورد بحث قرار می‌دهد و تهدیدات حساب‌های جعلی، سرقت هویت و نیز فیشینگ به طور خاص در شبکه‌های اجتماعی مورد بحث قرار می‌گیرد. در نهایت تلاش می‌کند تا دستورالعملی برای حفظ حریم خصوصی و تهدیدات فعلی آن در شبکه‌های اجتماعی ارائه دهد.	[61]

جدول ۳. مروری بر ادبیات موضوع

نویسنده	سال	هدف تحقیق	روش تحقیق	یافته‌ها	منبع
رائول پاردو و همکاران	۲۰۱۷	ارائه چارچوبی را برای نوشتن خط‌مشی‌های حفظ حریم خصوصی و استدلال درباره چنین سیاست‌هایی که شبکه را تکامل می‌دهند.	ارائه مدلی منطقی برای مشخص کردن ویژگی‌ها و استدلال درباره دانش کاربران و یک زبان رسمی برای نوشتن سیاست‌های حفظ حریم خصوصی.	توییتر و فیس‌بوک حریم خصوصی را حفظ نمی‌کنند.	[39]
سید محمد صفی و همکاران	۲۰۲۲	رفع چالش افشا و دسترسی غیرمجاز به اطلاعات، داده‌ها و ارتباط بین کاربران در شبکه‌های اجتماعی.	مدلی با رمزگذاری مبتنی بر ویژگی‌های خط‌مشی رمزنگاری (CP-ABE) و استاندارد رمزگذاری AES	طراحی ایمن و کلیدها به‌صورت امن مبادله می‌شوند.	[26]
خواکیم مارکزا و همکاران	۲۰۱۳	کنترل بیشتر کاربر بعد از قرارگیری داده‌ها بر روی شبکه‌ی اجتماعی	ارائه معماری مبتنی بر یک پلت فرم مدیریت حقوق باز که این معماری مکانیسم‌های امنیتی و حریم خصوصی لازم را اعمال می‌کند.	کاربران می‌توانند افشا و محافظت از محتوای خود را کنترل کنند	[40]
شوکت علی و همکاران	۲۰۱۸	ارائه توصیه‌هایی به کاربران شبکه‌های اجتماعی جهت افزایش حفظ حریم خصوصی آنها.	طرح سؤالات پرسش‌نامه‌ای، سؤالات در زمینه حفظ حریم خصوصی کاربران در شبکه‌های اجتماعی از بین دانشجویان کارشناسی.	عدم اطلاع بسیاری از کاربران در مورد تنظیمات حریم خصوصی	[41]
الکینی و همکاران	۲۰۱۴	جلوگیری از افشای اطلاعات حساس کاربران در شبکه‌های اجتماعی	ارائه مدلی از حفظ حریم خصوصی که توسط کاربر تنظیم می‌شود و مالک شبکه اجتماعی به آن نظارت می‌کند.	کاربران از مسائل حریم خصوصی آشنا نیستند، افزایش اعتماد به مالکان شبکه‌های اجتماعی	[42]
پاناگیوتیس و همکارانش	۲۰۱۵	حفظ حریم خصوصی در اشتراک‌گذاری تصاویر در شبکه‌های اجتماعی	با استفاده از فناوری تشخیص چهره جهت بلوری کردن تصاویر غیرمجاز.	عملکرد آن در ٪۸۷٫۳۵ رضایت بخش بوده است.	[25]
ژون یی و همکاران	۲۰۲۰	حفظ حریم خصوصی در تطبیق پروفایل در شبکه‌های اجتماعی	روشی بر اساس رمزگذاری هومومورفیک ساخته شده است و به کاربر این امکان را می‌دهد تا با کمک چندین سرور نمایه‌های مشابه کاربر را پیدا کند.	عملی‌بودن بر اساس آزمایش‌های انجام شده.	[43]
عرفان آقاسیان و همکاران	۲۰۱۷	اندازه‌گیری ریسک و افشای حریم خصوصی کاربران در چندین شبکه اجتماعی	با استفاده از سیستم‌های آماری و فازی، عوامل اصلی تأثیرگذار بر حریم خصوصی کاربران، یعنی حساسیت و دید را شناسایی می‌کند تا امتیاز افشای نهایی را برای هر کاربر به دست آورد.	تخمین بهتر از اندازه‌گیری افشای حریم خصوصی کاربران در چندین شبکه	[44]

نویسنده	سال	هدف تحقیق	روش تحقیق	یافته‌ها	منبع
				اجتماعی	
زایون هی و همکاران	۲۰۰۹	حفظ حریم خصوصی با استفاده از ناشناس‌سازی گراف	یک رویکرد ناشناس‌سازی آگاه از ساختار را پیشنهاد می‌کند که ساختار شبکه اصلی و همچنین ویژگی‌های ساختاری آن را درحالی‌که ناشناس می‌کند، حداکثر حفظ هم می‌کند.	فراهم شدن ناشناس‌سازی، اثربخشی و سودمندی عملی	[45]
کاه منگ و همکاران	۲۰۲۱	حفظ حریم خصوصی در تعقیب سایبری در شبکه‌های اجتماعی	دو مدل کلیدی حریم خصوصی تعریف شده است، یعنی عدم پیوند وزن لبه و عدم پیوندناپذیری گره برای جلوگیری از پیوند اطلاعات کمکی به یک فرد هدف با احتمال بالا.	حفظ حریم خصوصی در زمینه تعقیب سایبری.	[46]
شنگ هسو و همکاران	۲۰۱۴	حفظ حریم خصوصی در زمینه انتشار داده‌های شبکه اجتماعی.	یک چارچوب منطقی که می‌تواند مدل‌های حمله مختلف را به طور یکسان نشان دهد.	یکنواختی چارچوب زمینه مشترکی را برای مقایسه مدل‌های حمله موجود در اختیار قرار می‌دهد.	[47]
عبدالله الحصیب	۲۰۰۹	تهدیدات شبکه‌های اجتماعی	مزایای تجاری و اجتماعی استفاده ایمن و آگاهانه از شبکه‌های اجتماعی را برجسته می‌کند و بر مهم‌ترین تهدیدات برای کاربران تأکید می‌کند.	نشان‌دادن عوامل اساسی پشت تهدیدات، توصیه‌های فنی برای بهبود حریم خصوصی.	[48]
جیانلوکا لاکس و همکاران	۲۰۲۱	ارائه رویکرد غیرمتمرکز مبتنی بر بلاکچین برای مدیریت تنظیمات حریم خصوصی یک کاربر.	تغییرات در تنظیمات حریم خصوصی کاربر شبکه اجتماعی توسط یک قرارداد هوشمند تأیید می‌شود تا اطمینان حاصل شود که با انتظارات کاربران مطابقت دارد.	غیرمتمرکز و مبتنی بر اتریوم برای تأیید اثربخشی.	[49]
لارگو برونو	۲۰۲۰	ارائه روشی برای مدیریت مشکل کنترل دسترسی در شبکه‌های اجتماعی مبتنی بر بلاکچین.	مدلی ارائه می‌دهد که مبتنی بر بلاکچین به‌جای نقش محتوا نقش کاربر را به‌عنوان مرکز سیستم در نظر می‌گیرد.	بلاکچین به‌عنوان ابزاری برای مدیریت کنترل دسترسی	[50]

۲-۱- راه‌حل‌های حفظ حریم خصوصی در شبکه‌های اجتماعی

در چند سال گذشته، نقض حریم خصوصی در شبکه‌های اجتماعی توجه بسیاری از محققان در هر دو حوزه صنعتی و دانشگاهی را به خود جلب کرده است. راه‌حل‌های مختلفی برای مقابله با این تهدیدات پیشنهاد شده است. در این قسمت، در جدول ۴ روش‌ها و رویکردهای مختلفی که در مقالات مربوط به حریم خصوصی در شبکه‌های اجتماعی ارائه شده‌اند مورد بحث و بررسی قرار گرفته است.

جدول ۴: خلاصه ای از روش‌های جلوگیری از نقض حریم خصوصی در شبکه‌های اجتماعی[17]

راه‌حل	شرح	منابع
واترمارکینگ	روشی برای جاسازی داده‌ها در محتوای رسانه باهدف اثبات مالکیت محتوای رسانه است.	[5,6,7,8,9]
مالکیت مشترک	به کاربران متعددی اجازه می‌دهد تا سیاست‌های حفظ حریم خصوصی خود را بر روی فیلم‌ها، تصاویر مشترک با مالکیت مشترک اعمال کنند.	[10,11,12]
استگانالیز	مکانیزمی برای یافتن اطلاعات مخرب در داده‌های چندرسانه‌ای است.	[13,14,15]
رمزگذاری ذخیره‌سازی	اطلاعاتی را که در اختیار ارائه‌دهنده خدمات شخص ثالث مانند ارائه‌دهندگان خدمات ابری قرار می‌دهند، رمزگذاری شوند.	[16,18,19]
تشخیص بدافزار	مکانیسم‌های متفاوتی برای تشخیص انتشار بدافزار در شبکه‌های اجتماعی وجود دارد.	[20,21,22]
شناسایی پروفایل‌های جعلی و دفاعی سیبیل	ابزارها و تکنیک‌هایی برای شناسایی پروفایل‌های جعلی و دفاع در برابر حملات سیبیل ایجاد شده است. اکثر تکنیک‌ها به نمودارهای اجتماعی یا مفهوم مسیرهای تصادفی متکی هستند.	[23,24,28,29]
تشخیص اسپمر	رویکردهای موجود برای شناسایی اسپم در شبکه‌های اجتماعی استخراج یک مجموعه ویژگی است که کاربران اسپم را از افراد مجاز جدا کرده و آن ویژگی را به مدل‌های مختلف طبقه‌بندی کننده یادگیری ماشین برای شناسایی فعالیت‌های نامناسب ارائه می‌دهد.	[30,31,32,17]
راه‌حل‌های تجاری	توسط چندین شرکت امنیتی برای محافظت از کاربران شبکه‌های اجتماعی در برابر تهدیدات امنیتی تولید شده‌اند.	[17,33]
راه‌حل‌های داخلی در شبکه‌های اجتماعی	شبکه‌های اجتماعی راه‌حل‌های امنیتی داخلی مختلفی مانند تنظیمات حریم خصوصی کاربر، مکانیزم‌های مجوز را ارائه می‌دهند.	[34,35,17,36]
تشخیص شبیه‌سازی مشخصات	بسیاری از شبکه‌های اجتماعی ویژگی ای دارند که به‌صورت خودکار مشخصات شبیه‌سازی شده را شناسایی کرده و به کاربران در مورد چنین نمایه‌ای اطلاع می‌دهد.	[37,17,38]

۲-۲- شکاف ادبیات موضوع

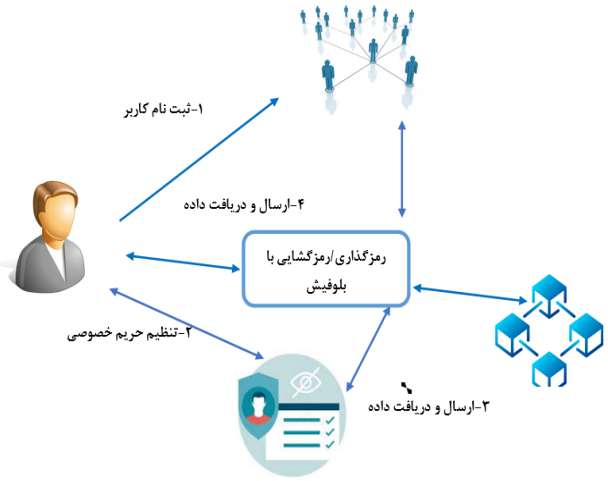
امروزه شبکه‌های اجتماعی به کاربران خود اجازه می‌دهند تا حریم خصوصی خود را خودشان تنظیم کنند البته در سال ۲۰۱۹ یک مطالعه انجام شده است که نشان می‌دهد بسیاری از کاربران نمی‌دانند و یا نمی‌توانند چگونه حریم خصوصی خود را تنظیم کنند[3].روش‌های مختلفی برای شناسایی افراد یا احراز هویت در شبکه‌های اجتماعی وجود دارد اما رایج‌ترین آنها استفاده از شماره همراه می‌باشد به‌طوری که ابتدا کاربر شماره همراه خود را وارد می‌کند و یک کد تایید برای او ارسال می‌شود و پس از ثبت‌نام می‌تواند با نام کاربری و رمزعبور وارد حساب کاربری خود شود. در روش پیشنهادی همین روش انجام شده است. اما تهدید برون سپاری و شفافیت مراکز داده یکی از تهدیدهای نقض حریم خصوصی در شبکه‌های اجتماعی محسوب می‌شود[17]. چرا که ممکن است داده‌های ارسالی ما در شبکه‌های اجتماعی مورد دستکاری قرار بگیرد یا داده‌های ما در شبکه‌های اجتماعی از طرف شرکت ارائه دهنده خدمات یا مالک شبکه‌اجتماعی بفروش برسد. برای جلوگیری از این کار ما در این تحقیق بلاکچین و برای رمزگذاری داده‌ها الگوریتم بلوفیش را پیشنهاد می‌کنیم.

۳- مدل پیشنهادی

در این بخش مدل پیشنهادی خود را تشریح می‌کنیم شکل ۱ نمای کلی مدل پیشنهادی را نشان می‌دهد.

استفاده از بلاکچین باعث می‌شود که مالک داده‌های تولید شده در شبکه‌های اجتماعی خود کاربر باشد و دیگر مالکین شبکه‌های اجتماعی قادر به دستکاری آنها و فروش آنها نیستند. یعنی شبکه اجتماعی کاربر محور می‌شود و هر کس مالک داده‌های خود است[51]. با توجه به اینکه در این مدل حفظ حریم خصوصی و اجرای دقیق و امن قراردادهای هوشمند از اهمیت بالایی برخوردار است روش مورد نظر ما برای ذخیره دادها در بلاکچین درون‌زنجیر[1] است.

الگوریتم گواه اثبات کار[2]، در حقیقت یک نوع الگوریتم اجماع است که از حملات DDoS و سایر سوءاستفاده‌ها در شبکه و همچنین از ایجاد اسپم در شبکه جلوگیری می‌کند. الگوریتم اثبات کار در بلاکچین و رمزارزها کاربردهای بسیار زیادی دارد.



شکل ۱. نمای کلی مدل پیشنهادی

به صورت کلی بلاکچین‌های مختلفی وجود دارد که هرکدام کاربردهایی دارند. بلاکچین عمومی معروف‌ترین است، به عنوان مثال می‌توان بیت‌کوین را به عنوان بلاکچین عمومی نام برد. بلاکچین‌های عمومی به شفافیت و امنیت شهرت دارند و هیچ نهادی وجود ندارد که شبکه را کنترل کند. اما بلاکچین خصوصی سریع‌تر است ولی امکان مشاهده و کنترل دادها به علت ماهیت خصوصی بودن آن وجود دارد [63]. Steemit یک شبکه اجتماعی مبتنی بر بلاکچین عمومی می‌باشد. در مدل پیشنهادی بلاکچین عمومی مدنظر است.

مزایا:

- بلاکچین می‌تواند مکانیسم‌های کنترل کاربر بهتری ایجاد کند
- حفظ تقریباً همه ابعاد حریم خصوصی
- غیرمتمرکز بودن، این امر باعث می‌شود که کاربران آزادی بیشتری داشته باشند و از سانسورها در امان باشند.
- مالکیت بر داده‌های شخصی و کنترل بهبودیافته بر محتوای تولید شده توسط کاربر
- بلاکچین می‌تواند امکانات جدیدی را برای شبکه‌های اجتماعی ارائه دهد. به عنوان مثال، این شبکه‌ها می‌توانند از قراردادهای هوشمند برای ایجاد اقتصادهای درون‌پلتفرمی و افزایش حریم خصوصی استفاده کنند.

معایب:

- ممکن است از تکنولوژی بلاکچین برای عملیات مجرمانه استفاده شود.
- سرعت پایین

۳-۱- عملکرد مدل پیشنهادی

در این قسمت عملکرد روش پیشنهادی که در شکل ۱ نمایش داده

[1] On-Chain

[2] Proof Of Work

شده است را به صورت گام به گام تشریح می‌کنیم:

۱. کاربران در شبکه اجتماعی ثبت‌نام می‌کنند.
برای ثبت‌نام کاربران ابتدا باید شماره تلفن همراه خود را احراز هویت کنند. پس از ثبت شماره تلفن همراه کاربران در شبکه اجتماعی، کد احراز هویت برای کاربر ارسال می‌شود که از طریق آن کاربر می‌تواند اصالت شماره تلفن همراه خود را اثبات کند. پس از تأیید شماره تلفن همراه کاربران، این شماره در پایگاه‌داده ذخیره می‌شود. شماره تلفن همراه کاربران به دلیل منحصربه‌فرد بودن، کاربران را از یکدیگر متمایز می‌کند. پایگاه‌داده شبکه اجتماعی یک پایگاه‌داده توزیعی بلاکچینی است که اطلاعات بر روی آن قرار می‌گیرد.

۲. تنظیم پروفایل
بعد از ثبت‌نام کاربر پروفایل خود را تنظیم می‌کند یعنی حریم خصوصی خود را تنظیم می‌کند. این بخش با استفاده از قراردادهای هوشمند انجام می‌شود. تنظیمات حریم خصوصی می‌تواند شامل: پنهان‌کردن استوری، مسدودسازی عده‌ای از کاربران و چه کسانی او را ببینند و دیگر اطلاعات مربوط به حریم خصوصی باشد.

۳. ذخیره حریم خصوصی تنظیم شده
حریم خصوصی تنظیم شده با الگوریتم بلوفیش رمز و جهت ذخیره به بلاکچین ارسال و آنجا ذخیره خواهد شد.

۴. ارسال و دریافت داده‌ها
حال کاربر به استفاده امن از شبکه اجتماعی مبتنی بر بلاکچین می‌کند. شایان‌ذکر است کلیه داده‌ها قبل از قرارگیری بر پایگاه‌داده با الگوریتم بلوفیش رمز می‌شوند.

۳-۲- روش رمزگذاری داده‌ها در مدل پیشنهادی

در این مدل قبل از اینکه داده‌ها بر روی دیتابیس بلاکچین قرار بگیرند با الگوریتم متقارن رمز می‌شوند. علت این امر این است که به هر دلیلی اگر داده‌های ما مورد حمله قرار گرفته‌اند (مانند حمله ۵۱ درصد) به داده‌ها آسیبی وارد نشود. روش رمزگذاری متقارن به این علت انتخاب شده است که سرعت بالاتری نسبت به نامتقارن دارد. البته روش‌های نامتقارن امنیتی بیشتری نسبت به متقارن دارد اما چون داده‌های ما توسط خود بلاکچین هش می‌شوند و خود بلاکچین امنیت را به شدت بالا می‌برد و در نتیجه سرعت برای ما حائز اهمیت است، به همین علت از متقارن استفاده کرده‌ایم.

انتخاب الگوریتم رمزگذاری به عوامل مختلفی از قبیل سرعت، امنیت، سادگی و ... بستگی دارد. در این مدل سرعت برای ما حائز اهمیت است، به همین علت الگوریتم رمزگذاری متقارنی که استفاده کرده‌ایم، بلوفیش است چراکه امنیت ما توسط بلاکچین به شدت حفظ می‌شود. با توجه به تحقیقات قبلی در عمل الگوریتم بلوفیش نسبت به دیگر الگوریتم‌های متقارن برای رمزگذاری فایل‌های تصویری سرعت بهتری نشان داده است[4,53,54,55,56,57]. البته الگوریتم‌های سریعتری هم نسبت به بلوفیش وجود دارد مثل ChaCha20 که ما از این الگوریتم به علت کوتاه‌تر بودن تاریخچه و محبوب نبودن آن نسبت به بلوفیش استفاده نکرده‌ایم. با توجه به این که در شبکه‌های اجتماعی از فایل‌های تصویری زیادی استفاده می‌شود ترجیح داده شد از این الگوریتم استفاده شود.

۳-۳- مدیریت کلید در مدل پیشنهادی

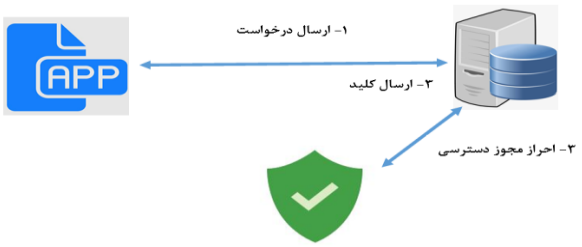
سروری که کلیدها بر روی آن قرار گرفته‌اند سروری است که تمام پروتکل‌های امنیتی بر روی آن اعمال شده است. کلیدها به‌صورت روزانه توسط سیستم تولید می‌شود و بر روی جدولی در پایگاه‌داده قرار می‌گیرند. یعنی پیام‌ها در هر روز با یک کلید متفاوت رمزگذاری می‌شوند و هنگام رمزگشایی باتوجه به تاریخ پیام با کلید آن روز رمزگشایی می‌شوند. شکل ۲ شمای کلی مدیریت کلید در مدل پیشنهادی را نشان می‌دهد. بدست آوردن کلید برای رمزگذاری و یا رمزگشایی در سه‌گام انجام می‌شود:

۱. درخواست کاربر از طریق برنامه به سرور کلیدها ارسال می‌شود.
۲. سرور درخواست را به سیستم احراز مجوز دسترسی ارسال می‌کند.
۳. سیستم احراز مجوز دسترسی درخواست را بررسی می‌کند درصورتی که درخواست احراز شد و مجوز دریافت کرد با توجه به تاریخ پیام کلید را انتخاب و درنهایت کلید را ارسال می‌کند.

۳-۴- امضای دیجیتال

امضای دیجیتال در سه‌گام انجام می‌شود:

۱. هش کردن
اولین گام هش کردن داده‌ها است. داده‌ها از طریق یک الگوریتم هش مانند SHA256 هش می‌شوند. اندازه یک پیام می‌تواند به طور قابل‌توجهی متفاوت باشد، اما پس از هش کردن، تمام مقادیر هش آن طول یکسانی خواهند داشت.



شکل ۲. مدیریت کلید در مدل پیشنهادی

۲. امضاء

پس از هش کردن داده‌ها، فرستنده پیام باید آن را امضاء کند. پیام با کلید خصوصی فرستنده امضا می‌شود و گیرنده پیام می‌تواند صحت پیام و امضاء فرستاده شده را با استفاده از کلید عمومی مربوطه که توسط امضاکننده ارائه شده، کنترل کند. هر دو کلید عمومی و خصوصی توسط فرستنده پیام تولید می‌شوند، اما فقط کلید عمومی با گیرنده به اشتراک گذاشته می‌شود. امضا دیجیتال در بلاکچین به طور مستقیم با محتوای هر پیام مرتبط است. بنابراین، هر پیام امضاء شده دیجیتال دارای امضای دیجیتال متفاوتی خواهد بود. امضایی که هیچ‌کس نمی‌تواند آن را جعل کند.

۳. تأیید

فرایند تأیید زمانی اتفاق می‌افتد که گیرنده با استفاده از کلید عمومی ارائه شده توسط فرستنده دریافت پیام و اعتبارسنجی امضاء را تأیید کند. گام‌های فوق در شکل ۳ و ۴ نمایش داده شده است.

۴- ارزیابی

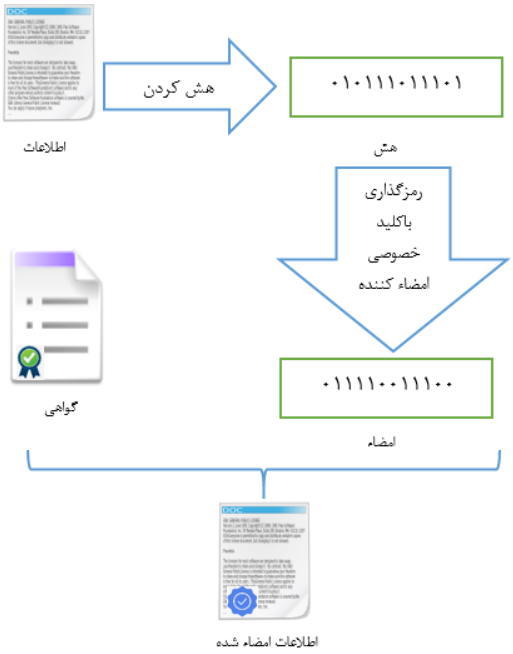
در این قسمت به اجرای تحقیق و ارزیابی روش پیشنهادی خود می‌پردازیم.

۴-۱- ارزیابی حفظ حریم خصوصی

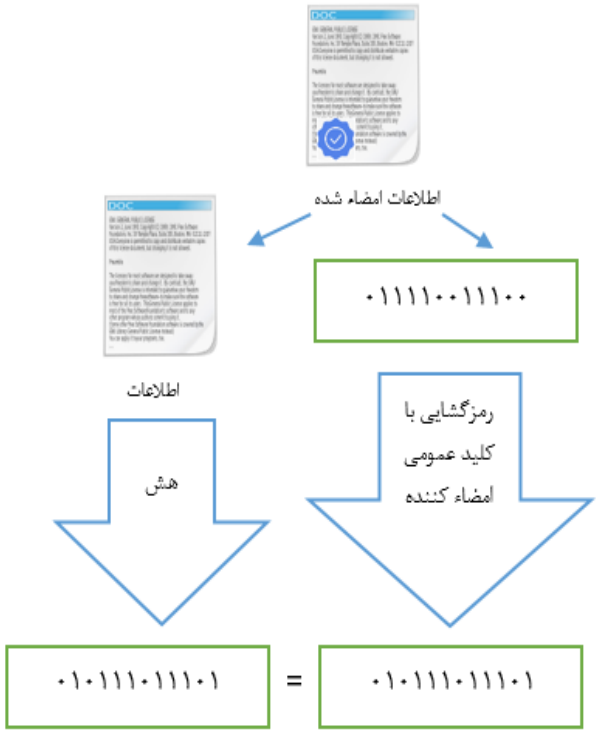
عناصر مهم حریم خصوصی شامل محرمانه بودن داده‌ها، کنترل دسترسی دقیق است[26]. روش پیشنهادی به طور کامل هر دو عنصر را فراهم می‌کند:

- **محرمانه بودن داده‌ها:**

با توجه به این که مدل پیشنهادی از فناوری بلاکچین استفاده می‌کند و این فناوری برای ایجاد امنیت بیشتر از اساس به‌گونه‌ای طراحی شده است که برای تأیید یا ذخیره هر داده، به اعتبارسنجی نودهای مختلف شبکه احتیاج می‌باشد که از ویژگی‌های مهم برای امن نگه‌داشتن بلاکچین است. به این صورت یک عامل مخرب نمی‌تواند با دسترسی پیداکردن به پایگاه‌داده اطلاعات ذخیره شده آن را مختل کند یا تغییر دهد، در نتیجه اطلاعات ثبت شده در شبکه بلاکچین به علت نیاز به امضای نودها برای تغییر، به‌نوعی تغییرناپذیر محسوب می‌شوند. اساس بلاکچین بر پایه رمزنگاری و حفظ امنیت اطلاعات بنا شده است و برای انتقال داده‌ها در آن از ویژگی هشینگ استفاده می‌شود و ما در این مدل قبل از هش داده‌ها ابتدا آنها را با الگوریتم بلوفیش رمز می‌کنیم و بعد رمز توسط بلاکچین با تابع هش SHA256 هش می‌شود. در هش هرگز امکان ندارد دو هش یکسان برای اطلاعات متفاوت ایجاد شود.



شکل ۳. فرایند امضاء



شکل ۴. فرایند تایید

برای ساخت هر بلاک در بلاکچین نیز از هش بلاک قبل استفاده می‌شود و اگر شخصی (عامل مخرب) قصد ایجاد تغییر در اطلاعات ذخیره شده قبلی را داشته باشد، مجبور می‌شود تمام بلاک‌های بعد از آن را نیز از نو بسازد و هش کند. به علت این ویژگی فناوری بلاکچین، خرابکاری وی بلافاصله لو می‌رود.

به عنوان مثال فرض کنید کاربر A می‌خواهد پیام "سلام" را به کاربر B ارسال کند مراحل آن در شکل ۵ شرح داده شده است. برای نمایش سلام برای کاربر B مراحل شکل ۶ طی می‌شود.

با اجرای مراحل فوق و با استفاده از بلاکچین توانسته‌ایم داده‌های خود را نامتمرکز کنیم که این باعث می‌شود مالکان شبکه‌های اجتماعی نتوانند از داده‌های کاربران سوءاستفاده کنند.

با توجه به ذخیره‌سازی داده‌ها در بلاکچین و استفاده از مکانیزم‌های هش و رمزگذاری اگر کاربری قصد دستکاری پیام داشته باشد و به هر دلیلی موفق هم شود چون هش بلاک در بلاک قبلی است و با تغییر پیام توسط عامل مخرب، هش تغییر می‌کند و برای همه قابل مشاهده است که این پیام تغییر کرده است و به همین علت کاربر غیرمجاز امکان دستکاری در پیام را ندارد.

به عنوان مثال فرض کنید بلاک‌های شکل ۷ را داریم و کاربری قصد تغییر اطلاعات بلاک شماره ۲ را دارد و فرض می‌کنم می‌تواند این کار را انجام دهد زمانی که این کار را انجام می‌دهد هش بلاک تغییر می‌کند و با هش بلاک ۳ که هش بلاک قبلی را نگهداری می‌کند همخوانی ندارد و همه متوجه می‌شوند این بلاک تغییر پیدا کرده است.

- **کنترل دقیق دسترسی:**

مدل پیشنهادی با استفاده از قراردادهای هوشمند در بلاکچین کنترل دقیق دسترسی‌ها را انجام می‌دهد به عنوان مثال اگر یک کاربر یک کاربر دیگر را مسدود کرده باشد این کار با استفاده از قراردادهای هوشمند به درستی انجام می‌شود.

۴-۲- مقایسه طرح پیشنهادی با طرح‌ها دیگر

در این بخش، طرح پیشنهادی ما از عناصر حفظ حریم خصوصی و حملات متداول مانند حملات اختلال سرویس، حفاظت از داده‌ها در برابر مالکان شبکه‌های اجتماعی، تبادل کلید امن، رمزگذاری داده‌ها، کنترل دسترسی دقیق، برنامه متن‌باز، اطلاعات درهم‌سازی شده، غیرمتمرکز بودن و رمزگذاری سرتاسر با سایر طرح‌ها مقایسه شده است. نتیجه مقایسه در جدول ۴ نشان داده شده است.

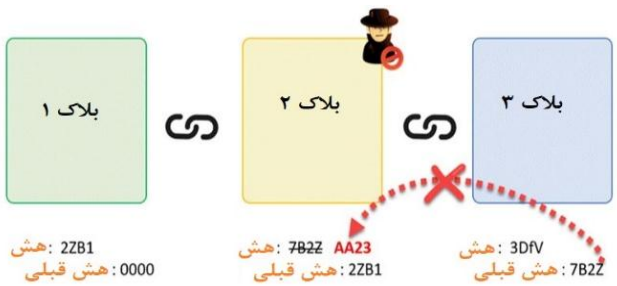
۴-۳- ارزیابی عملکرد روش پیشنهادی

برای شبیه‌سازی یک برنامه‌ای را با استفاده از زبان سی‌شارپ پیاده‌سازی کرده‌ایم تا بتوانیم زمان رمزگذاری و رمزگشایی را محاسبه کنیم با استفاده از این می‌توانیم متن و تصاویر را رمزگذاری کنیم ما چند سناریوی زیر را برای شبیه‌سازی انجام می‌دهیم لازم به ذکر است شبیه‌سازی بر روی یک دستگاه با مشخصات زیر اجرا شده است:

CPU:AMD FX-7600P Radeon R7, 12 Compute Cores 4C+8G 2.70 GHz, RAM:8GB

شکل ۵. ارسال اطلاعات از کاربر A به کاربر B

شکل ۶. نمایش پیام برای کاربر B



شکل ۷. تغییر اطلاعات توسط کاربر مخرب.[52]

گام‌های الگوریتم به شرح ذیل می‌باشند:

۱- دریافت داده برای رمزگذاری/رمزگشایی.
۲- دریافت کلید از سرور کلیدها برای رمزگذاری/رمزگشایی.
۳-رمزگذاری/رمزگشایی داده‌ها.

شبه‌کد مربوطه در شکل ۸ نمایش داده شده است.

```
static void Main()
{
string dataToEncryptDecrypt = "Your data to encrypt";
byte[] keyFromServer = GetKeyFromServer();
byte[] encryptedOrDecryptedData =
EncryptOrDecryptedDataWithBlowFish(dataToEncryptDecr
ypt, keyFromServer);
}
```

GetKeyFromServer().یک تابع برای دریافت کلید از سرور کلیدها است:

EncryptOrDecryptedDataWithBlowFish : متدی که وظیفه‌ی رمزگذاری و رمزگشایی داده‌ها با الگوریتم بلوفیش را دارد.

شکل ۸. شبه‌کد الگوریتم رمزگذاری و رمزگشایی

جدول ۴. مقایسه مدل پیشنهادی با دیگر طرح‌ها

	[25]	[43]	[46]	[26]	مدل پیشنهادی
مقاوم در برابر حملات اختلال سرویس	خیر	خیر	خیر	خیر	بله
جلوگیری از ذخیره داده در سرورها	خیر	خیر	خیر	خیر	بله
رمزگذاری داده‌ها	-	بله	-	بله	بله
حفاظت داده در برابر مالک شبکه اجتماعی	بله	خیر	خیر	خیر	بله
محرمانه بودن داده‌ها	خیر	بله	بله	بله	بله
اطلاعات درهم‌سازی شده	خیر	خیر	خیر	خیر	بله
غیرمتمرکز بودن	خیر	خیر	خیر	خیر	بله
تبادل کلید امن	-	بله	-	بله	بله
کنترل دسترسی دقیق	خیر	بله	بله	بله	بله
رمزگذاری سرتاسر	خیر	خیر	خیر	بله	خیر

سناریوی زیر برای متن در نظر گرفته شده است:

۱-زمان رمزگذاری متن با حجم صفر کیلوبایت تا ۸ کیلوبایت برابر است با ۴ تا ۷ میلی ثانیه

۲- زمان رمزگشایی متن با حجم صفر کیلوبایت تا ۸ کیلوبایت برابر است با ۴ تا ۶ میلی ثانیه

۳-زمان رمزگذاری متن با حجم ۹ کیلوبایت تا ۲۳ کیلوبایت برابر است با ۸ تا ۱۷ میلی ثانیه

۴-زمان رمزگشایی متن با حجم ۹ کیلوبایت تا ۲۳ کیلوبایت برابر است با ۷ تا ۱۴ میلی ثانیه

۵-زمان رمزگذاری متن با حجم ۲۴ کیلوبایت تا ۴۴ کیلوبایت برابر است با ۱۸ تا ۳۷ میلی ثانیه

۶-زمان رمزگشایی متن با حجم ۲۴ کیلوبایت تا ۴۴ کیلوبایت برابر است با ۱۵ تا ۲۵ میلی ثانیه

خروجی آن در شکل ۹ نمایش داده شده است.

سناریوی زیر برای تصاویر در نظر گرفته شده است:

۱-زمان رمزگذاری تصاویر با حجم ۰کیلوبایت تا ۵کیلوبایت برابر است با ۴ تا ۷ میلی ثانیه

۲-زمان رمزگشایی تصاویر با حجم ۰کیلوبایت تا ۵کیلوبایت برابر است با ۴ تا ۶ میلی ثانیه

۳-زمان رمزگذاری تصاویر با حجم ۶ کیلوبایت تا ۱۹ کیلوبایت برابر است با ۸ تا ۱۷ میلی ثانیه

۴- زمان رمزگشایی تصاویر با حجم ۶ کیلوبایت تا ۱۹ کیلوبایت برابر است با ۷ تا ۱۶ میلی ثانیه

۵-زمان رمزگذاری تصاویر با حجم ۲۰ کیلوبایت تا ۷۵ کیلوبایت برابر است با ۱۸ تا ۵۵ میلی ثانیه

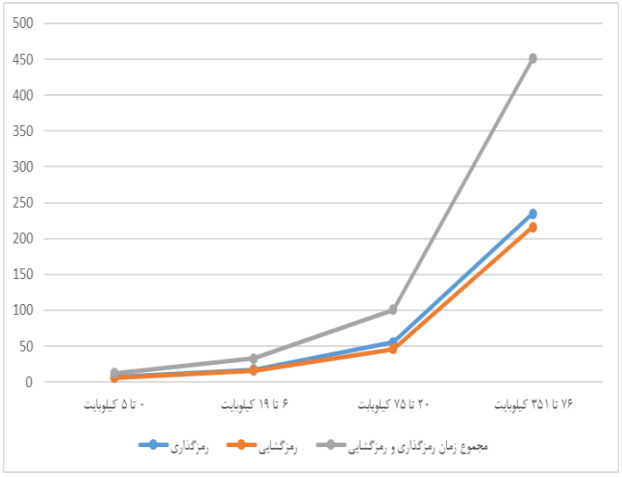
۶- زمان رمزگشایی تصاویر با حجم ۲۰ کیلوبایت تا ۷۵ کیلوبایت برابر است با ۱۷ تا ۴۶ میلی ثانیه

۷-زمان رمزگذاری تصاویر با حجم ۷۶ کیلوبایت تا ۳۵۱ کیلوبایت برابر است با ۵۶ تا ۲۳۵ میلی ثانیه

۸- زمان رمزگشایی تصاویر با حجم ۷۶ کیلوبایت تا ۳۵۱ کیلوبایت برابر است با ۴۷ تا ۲۱۶ میلی ثانیه

خروجی آن در شکل ۱۰ نمایش داده شده است.

شکل ۹. زمان رمزگذاری و رمزگشایی متن بر حسب میلی ثانیه



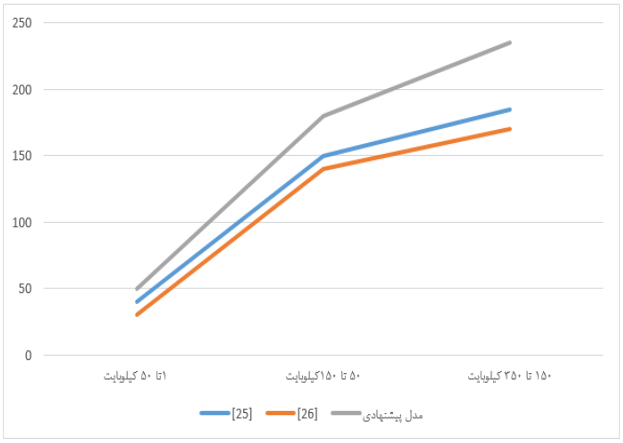
شکل ۱۰. زمان رمزگذاری و رمزگشایی تصاویر بر حسب میلی ثانیه

در این مدل باتوجه به اینکه ما از بلاکچین استفاده می‌کنیم حفظ حریم خصوصی کاربران تا حد بسیار زیادی افزایش پیدا می‌کند ضمن اینکه قبل از ذخیره داده در بلاکچین توسط الگوریتم بلوفیش رمز می‌شود و بعد از هش در بلاکچین ذخیره می‌شود.

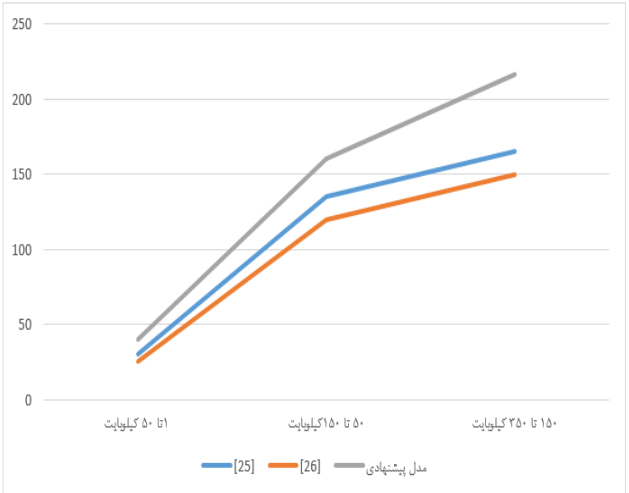
۴-۴- مقایسه طرح پیشنهادی با طرح‌های دیگر از نظر عملکرد و کارایی

در این بخش مدل پیشنهادی خود را با دو طرح دیگر از نظر زمان رمزگذاری و رمزگشایی مقایسه کرده‌ایم که نتایج آن در شکل ۱۱ و ۱۲ نشان داده شده است.

زمان رمزگذاری و رمزگشایی مدل پیشنهادی با دو طرح مقایسه شده بیشتر است. اما حفاظت بیشتری از حریم خصوصی انجام می‌دهد و با توجه به اینکه قبل از ذخیره‌سازی داده‌ها در بلاکچین، داده‌ها رمزگذاری می‌شوند و سپس بلاکچین هش می‌شوند و بعد در پایگاه‌داده بلاکچینی ذخیره می‌شوند حفاظت از حریم خصوصی بسیار بالا می‌رود و در نتیجه مدل پیشنهادی از حریم خصوصی نسبت به دو مدل مقایسه شده حفاظت بهتری می‌کند.



شکل ۱۱. زمان رمزگذاری برحسب میلی ثانیه



شکل ۱۲. زمان رمزگشایی برحسب میلی ثانیه

۵- نتیجه گیری

شبکه‌های اجتماعی به یک رسانه ارتباطی مطلوبی برای میلیاردها کاربر وب تبدیل شده‌اند، به‌طوری‌که چنین سرویس‌هایی به مردم اجازه می‌دهند تا علایق، عکس‌ها، ویدئوها را به اشتراک بگذارند امروزه خیلی از کاربران شبکه‌های اجتماعی از این طریق کسب درآمد می‌کنند، شبکه‌های اجتماعی امروزه با کسب‌وکارها پیوند زده شده‌اند. اما این خدمات می‌توانند کاربران را در معرض خطرات جدی نقض حریم خصوصی قرار دهند. یکی از مهم‌ترین و بزرگترین مشکلات موارد نقض حریم خصوصی فروش و یا به‌اشتراک‌گذاری داده‌ها توسط مالکان شبکه‌های اجتماعی است که در این تحقیق روشی ارائه دادیم مبتنی بر بلاکچین و رمزنگاری تا از این نقض حریم خصوصی کاربران جلوگیری کند مدل پیشنهادی با چند طرح دیگر مقایسه و ارزیابی شد و نشان داده شد که مدل پیشنهادی ما سرعت رمزگذاری و رمزگشایی کمتری (کندتر) نسبت به طرح‌های مقایسه شده دارد اما رعایت و حفظ حریم خصوصی در طرح پیشنهادی ما نسبت به طرح‌های مقایسه شده بیشتر است. از محدودیت‌های طرح ما می‌توان به‌سرعت اینترنت مناسب برای اجرای صحیح طرح پیشنهادی که باید حداقل 4G یا بالاتر یا معادل آن باشد و همین‌طور دستگاه تلفن همراهی که این روش را به‌خوبی پشتیبانی می‌کند باید حداقل یک دستگاه متوسط از نظر سخت‌افزاری باشد.

در تحقیقات آینده ما سعی خواهیم کرد از طرح پیشنهادی و یا ترکیب بلاکچین و سیستم‌های متمرکز به عنوان درون‌زنجیر و برون‌زنجیر، برای طراحی و پیاده‌سازی یک پلتفرم شبکه اجتماعی غیرمتمرکز و مبتنی بر بلاکچین استفاده کنیم.

مراجع

[1] H. Gao , J. Hu , T. Huang , J. Wang , Y. Chen ,"Security issues in online social networks", *IEEE Internet Computer*, Vol. 15(4), pp. 56–63, July-Aug. 2011, DOI: 10.1109/MIC.2011.50.

[2] M. Fire , R. Goldschmidt , Y. Elovici , "Online social networks: threats and solutions", *IEEE Communications Surveys & Tutorials*,vol. 16 (4),pp. 5-15, 02 May 2014, DOI: 10.1109/COMST.2014.2321628.

[3] Gianluca Lax , Antonia Russo, Lara Saidia Fascì, "A Blockchain-based approach for matching desired and real privacy settings of social network users", *Information Sciences*, vol. 557, pp. 220-235, May 2021,DOI: https://doi.org/10.1016/j.ins.2021.01.004 .

[4] Diaa Salama Abd Elminaam, Hatem Mohamed Abdual Kader, and Mohiy Mohamed Hadhoud , "Evaluating The Performance of Symmetric Encryption Algorithms", *IJCSNS International Journal of Computer Science and Network Security*, VOL.8 No.12, December 2008, May 2010

[5] [۵] A.M. Alattar, N.D. Memon, C.D. Heitzenrater, "Media Watermarking", Available: https://www.spiedigitallibrary.org/proceedings/Download?urlId=10.1117%2F12.2022495

[6] A. Zigomitros, A. Papageorgiou, C. Patsakis, "Social network content management through watermarking", *in: Proceedings of the 11th International Conference on Trust, Security and Privacy in Computing and Communications, IEEE*, 25-27 June 2012, DOI: 10.1109/TrustCom.2012.264

[24] G. Wang, F. Musau, S. Guo, M.B. Abdullahi, "Neighbor similarity trust against sybil attack in P2P e-commerce", *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, pp. 824-833, March 2015,doi: 10.1109/TPDS.2014.2312932

[25] Panagiotis Ilia, Iasonas Polakis, Elias Athanasopoulos, Federico Maggi, Sotiris Ioannidis,"Preventing Privacy Leakage From Photos in Social Networks", *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*,pp. 781-792, October 2015,doi: https://doi.org/10.1145/2810103.2813603

[26] Seyyed Mohammad Safi, Ali Movaghar, Mohammad Ghorbani,"Privacy protection scheme for mobile social network", *Journal of King Saud University - Computer and Information Sciences*, vol.34, pp. 4062-4074, july 2022, doi:https://doi.org/10.1016/j.jksuci.2022.05.011

[27] Sun, X., Yao, Y., Xia, Y., Liu, X., Chen, J., Wang, Z., 2016. "Towards Efficient Sharing of Encrypted Data in Cloud-Based Mobile Social Network". *KSII Transactions on Internet and Information Systems* , VOL. 10, NO. 4,pp. 1892–1903, Apr. 2016

[28] N. Tran, J. Li, L. Subramanian, S.S. Chow, "Optimal sybil-resilient node admission control", *Proceedings of the INFOCOM IEEE*, 10-15 April 2011 ,doi: 10.1109/INFCOM.2011.5935171

[29] W. Wei, F. Xu, C.C. Tan, Q. Li, "SybilDefender: a defense mechanism for Sybil attacks in large social networks", *IEEE Trans*,vol. 24,pp. 2492-2502, December 2013,doi: 10.1109/TPDS.2013.9

[30] A. Hai Wang, "Don't follow me: spam detection in twitter", *Proceedings of the International Conference on Security and Cryptography (SECRYPT) IEEE*, 26-28 July 2010.

[31] F. Ahmed, M. Abulaish, "A generic statistical approach for spam detection in Online Social Networks", *Computer Communications*,vol. 36,pp. 1120-1129, June 2013, doi: https://doi.org/10.1016/j.comcom.2013.04.004

[32] H. Gao, Y. Chen, K. Lee, D. Palsetia, A.N. Choudhary, "Towards online spam filtering in social networks", 2012

[33] M. Fire, R. Goldschmidt, Y. Elovici, "Online social networks: threats and solutions", *IEEE Communications Surveys & Tutorials*,vol. 16,pp. 2019-2036, 02 May 2014,doi: 10.1109/COMST.2014.2321628

[34] D.H. Lee, "Personalizing information using users' online social networks: a case study of CiteULike", *Journal of Information Processing Systems*,vol. 11,pp. 1, 2015,doi: 10.3745/JIPS.04.0014

[35] D. Wang, N. Wang, P. Wang, S. Qing, "Preserving privacy for free: efficient and provably secure two-factor authentication scheme with user anonymity", *Information Sciences* ,vol. 321,pp.162-178, 10 November 2015,doi: https://doi.org/10.1016/j.ins.2015.03.070

[36] T. Stein, E. Chen, K. Mangla, "Facebook immune system", *Proceedings of the 4th Workshop on Social Network Systems*, No. 8 ,pp. 1-8, April 2011,doi: https://doi.org/10.1145/1989656.1989664

[37] G. Kontaxis, I. Polakis, S. Ioannidis, E.P. Markatos, "Detecting social network profile cloning", *Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops) IEEE*, 21-25 March 2011, DOI: 10.1109/PERCOMW.2011.5766886

[38] Z. Shan, H. Cao, J. Lv, C. Yan, A. Liu, "Enhancing and identifying cloning attacks in online social networks", *Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication*,NO. 59,pp. 1-6, January 2013, doi: https://doi.org/10.1145/2448556.2448615

[39] Raúl Pardo a, Musard Balliu a, Gerardo Schneider, "Formalising privacy policies in social networks, Journal of Logical and Algebraic Methods in Programming", *Journal of Logical and Algebraic Methods in Programming* ,vol. 90,pp. 125-157, August 2017,doi: https://doi.org/10.1016/j.jlamp.2017.02.008

[40] Joaquim Marquesa, Carlos Serrãob, "Improving content privacy on social networks using open digital rights management solutions", *Procedia Technology*, vol. 9, pp. 405-410, 2013,doi: https://doi.org/10.1016/j.protcy.2013.12.045

[7] C. Ho Sin, N.A. Kim, B.W. Go, K.S. Min, J.D. Lee, J.H. Park, "Realizing the Right to Be Forgotten in an SNS Environment", Advances in Computer Science and its Applications, vol. 279, pp. 1443-1449, (2014)

[8] C. Patsakis, A. Zigomitros, A. Papageorgiou, E. Galván-López, "Distributing privacy policies over multimedia content across multiple online social networks" *Computer Networks*,vol. 75, pp. 531-543, 24 December 2014, DOI: https://doi.org/10.1016/j.comnet.2014.08.023.

[9] K. Thongkor, N. Mettripun, T. Pramoun, T. Amornraksa, "Image watermarking based on DWT coefficients modification for social networking services", *in: Proceedings of the 10th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON) IEEE*, 15-17 May 2013, DOI: 10.1109/ECTICon.2013.6559626

[10] A.C. Squicciarini, H. Xu, X.L. Zhang, "CoPE: enabling collaborative privacy management in online social networks", *J. Am. Soc. Inf. Sci. Technol*,vol. 62, 25 January 2011,DOI: https://doi.org/10.1002/asi.21473

[11] A.C. Squicciarini, M. Shehab, J. Wede, "Privacy policies for shared content in social network sites", *VLDB J*,vol. 19,pp. 779-796, 30 June 2010.

[12] H. Hu, G.J. Ahn, J. Jorgensen, "Multiparty access control for online social networks: model and mechanisms", *IEEE Trans*,vol. 25,pp.1614-1627, 7 July 2013 ,DOI: 10.1109/TKDE.2012.97

[13] F. Li, K. Wu, J. Lei, M. Wen, Z. Bi, C. Gu, "Steganalysis over large-scale social networks with high-order joint features and clustering ensembles", *IEEE Trans* Inf Forensic Secur, vol. 11, pp. 344-357, 2 February 2016 ,DOI: 10.1109/TIFS.2015.2496910

[14] N. Venkatachalam, R. Anitha, "A multi-feature approach to detect Stegobot: a covert multimedia social network botnet", *Multimed Tools Appl* ,vol. 76,pp. 6079-6096,2017, DOI: 10.1007/s11042-016-3555-3

[15] V. Natarajan, S. Sheen, R. Anitha, "Multilevel analysis to detect covert social botnet in multimedia social networks", *IEEE Comput*,vol. 58,pp. 679-687, April 2015,DOI: 10.1093/comjnl/bxu063

[16] M. Tierney, I. Spiro, C. Bregler, L. "Subramanian, Cryptagram: photo privacy for online social media", *Proceedings of the first ACM conference on Online social networks*, pp. 75-88, October 2013,doi: https://doi.org/10.1145/2512938.2512939

[17] S. Rathore, P. Kumar Sharma, V. Loia , Y. Jeong, J. Park , "Social network security: Issues, challenges, threats, and solutions" , *Information Sciences*,vol. 421,pp. 43-69, December 2017,doi: https://doi.org/10.1016/j.ins.2017.08.063.

[18] P. Savla, L.D. Martino, "Content analysis of privacy policies for health social networks", *Proceedings of the International Symposium on Policies for Distributed Systems and Networks* 16-18 July 2012 , DOI: 10.1109/POLICY.2012.20

[19] X. Liu, Q. Liu, T. Peng, J. Wu, "Dynamic access policy in cloud-based personal health record (PHR) systems", *Inf. Sci*,vol. 379,pp. 62-81, 10 February 2017,doi: https://doi.org/10.1016/j.ins.2016.06.035

[20] G. Yan, G. Chen, S. Eidenbenz, N. Li, "Malware propagation in online social networks: nature, dynamics, and defense implications"*Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, vol. 7 ,pp. 196-206, March 2011, doi: https://doi.org/10.1145/1966913.1966939

[21] H. Zhu, C. Huang, H. Li, "MPPM: Malware propagation and prevention model in online social network", *IEEE International Conference on Communications Workshops (ICC)*, 10-14 June 2014,doi: 10.1109/ICCW.2014.6881278

[22] W. Xu, F. Zhang, S. Zhu, "Toward worm detection in online social networks", *Proceedings of the 26th Annual Computer Security Applications Conference*,pp. 11-20, December 2010, doi: https://doi.org/10.1145/1920261.1920264

[23] G. Danezis, P. Mittal, SybilInfer: "detecting sybil nodes using social networks", *NDSS*, 2009

[53] Aamer Nadeem, Dr M. Younus Javed," A Performance Comparison of Data Encryption Algorithms", *International Conference on Information and Communication Technologies*, 27-28 August 2005,doi: 10.1109/ICICT.2005.1598556

[54] D. Commey,S. Griffith Klogo,J. Dzisi Gadze," Performance comparison of 3DES, AES, Blowfish and RSA for Dataset Classification and Encryption in Cloud Data Storage",*International Journal of Computer Applications*,vol. 177, February 2020

[55] Chandrashekhar B,Dr. Mohamed Abdul Waheed," Analysis of Possible Attacks on Data and Possible Solutions with Comparative Analysis of Various Encryption Algorithms and Evaluation", *International Journal of Innovative Research in Engineering & Management (IJIREM)*,vol. 9, April 2022,doi: https://doi.org/10.55524/ijirem.2022.9.2.7

[56] C. Rathod,A. Gonsai," Performance Analysis of AES, Blowfish and Rijndael: Cryptographic Algorithms for Audio", *Rising Threats in Expert Applications and Solutions*, pp. 203–209,02 October 2020, doi: 10.1007/978-981-15-6014-9_24

[57] H. Alabdulrazzaq, M. Alenezi," Performance Analysis and Evaluation of Cryptographic Algorithms: DES, 3DES, Blowfish, Twofish, and Threefish ", *International Journal of Communication Networks and Information Security (IJCNIS)*,vol. 14, No. 1, April 2022

[58] Bin Zhou ,Jian Pei," Preserving Privacy in Social Networks Against Neighborhood Attacks ", *IEEE 24th International Conference on Data Engineering*, 07-12 April 2008,doi: 10.1109/ICDE.2008.4497459

[59] A.Jain,S.Ranjan Sahoo,J.Kaubiyal," Online social networks security and privacy: comprehensive review and analysis ", *Complex & Intelligent Systems*, Vol. 7, pp. 2157–2177, 01 June 2021,doi: 10.1007/S40747-021-00409-7

[60] Seyed Hossein Mousavi , Hamid Barati," SECURITY AND PRIVACY IN SOCIAL NETWORKS ", *Journal of Positive School Psychology*, Vol. 6, No. 5 ,2022

[61] Ahmed Al-Charchafchi, S. Manickam,Zakaria N. M. Alqattan," Threats Against Information Privacy and Security in Social Networks: A Review ", *Springer Nature Singapore Pte Ltd*, pp. 358–372, 2020,doi: https://doi.org/10.1007/978-981-15-2693-0_26

[62] R. Malekhosseini, M. Hosseinzadeh,K. Navi," An investigation into the requirements of privacy in social networks and factors contributing to users' concerns about violation of their privacy ", *Social Network Analysis and Mining*,11 june 2018,doi: https://doi.org/10.1007/s13278-018-0518-x

[63] P.K. Paul, P.S. Aithal, R.Saavedra, Su. Ghosh, "Blockchain Technology and its Types—A Short Review ", *International Journal of Applied Science and Engineering*, December 2021

[41] Shaukat Ali ,Naveed Islam , Azhar Rauf , Ikram Ud Din and Mohsen Guizani and Joel J. P. C. Rodrigues, "Privacy and Security Issues in Online Social Networks",*future internet*,2018

[42] Nader Yahya Alkeinaya, Norita Md. Norwawi, User Oriented Privacy Model for Social Networks, *Procedia - Social and Behavioral Sciences*,vol. 129,pp. 191-197 , 15 May 2014,doi: https://doi.org/10.1016/j.sbspro.2014.03.666

[43] Xun Yi, Elisa Bertino, Fang-Yu Rao, Kwok-Yan Lam, Surya Nepal and Athman Bouguettaya, "Privacy-Preserving User Profile Matching in Social Networks" *IEEE*,vol. 32,pp. 1572-1585, 01 August 2020,doi: 10.1109/TKDE.2019.2912748

[44] Erfan Aghasian, Saurabh Garg, (Member, IEEE), Longxiang Gao, (Member, IEEE), Shui Yu, Senior Member, IEEE) and James Montgomery, (Member, IEEE) , "Scoring Users' Privacy Disclosure Across Multiple Online Social Networks", *IEEE Access*,vol. 5, 27 June 2017,doi: 10.1109/ACCESS.2017.2720187

[45] Xiaoyun He, Jaideep Vaidya, Basit Shafiq, Nabil Adam, Vijay Atluri, "Preserving Privacy in Social Networks: A Structure-Aware Approach", *2009 IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology*, Milan, Italy, 15-18 September 2009,doi: 10.1109/WI-IAT.2009.108

[46] KAH MENG CHONG AND AMIZAH MALIP, "Trace Me If You Can: An Unlinkability Approach for Privacy-Preserving in Social Networks", *IEEE Access*,vol. 9,pp. 143950 - 143968 , 17 March 2021,doi: 10.1109/ACCESS.2021.3066176

[47] Tsan-sheng Hsu, Churn-Jung Liau ,Da-Wei Wang, "A logical framework for privacy-preserving social network publication", *Journal of Applied Logic*,vol.12,pp. 151-174,june 2014,doi: https://doi.org/10.1016/j.jal.2013.12.001

[48] Abdullah Al Hasib, "Threats of Online Social Networks", *International Journal of Computer Science and Network Security*,vol. 9, November 2009.

[49] Gianluca Lax , Antonia Russo, Lara Saidia Fascì, "A Blockchain-based approach for matching desired and real privacy settings of social network users", *Information Sciences*,vol.557,pp. 220-235,may 2021,doi: https://doi.org/10.1016/j.ins.2021.01.004

[50] Largo Bruno Pontecorvo, "When Blockchain meets Online Social Networks", *Pervasive and Mobile Computing*,vol. 62,pp. 101-131, February 2020,doi: https://doi.org/10.1016/j.pmcj.2020.101131

[51] Le Jiang , Xinglin Zhang, "A Blockchain-Based Decentralized Online Social Network", *IEEE TRANSACTIONS ON COMPUTATIONAL SOCIAL SYSTEMS*, VOL. 6, pp. 1454-1466, DECEMBER 2019,doi: 10.1109/TCSS.2019.2941650

[52] https://www.guru99.com